

The Applicant has recognized that this paradigm of ubiquitous computer terminals is likely to introduce problems in a typical networked environment, particularly with regard to providing secure communications via these terminals, and has disclosed and claimed solutions to these anticipated problems.

With regard to claim 5, and thereby dependent claims 6-8, the Applicant specifically claims that the user's private key is destroyed after use. The Examiner acknowledges that Trostle fails to teach destroying any record of the private key at the location of the user. The Examiner asserts, however, that Asay teaches the destruction of the user's private key, and that the combination of Asay and Trostle leads to the Applicant's invention. The Applicant respectfully traverses this assertion.

The entire premise of Trostle's invention is a security system that is "*transparent to the user*" (Trostle's Summary of the Invention, column 3, lines 23-30). The entire premise of the Applicant's invention is to assure *the presence of the user, by requiring* the user to initiate some identifying action for each security transaction. If the user's private key is destroyed, as taught and claimed by the Applicant, the user must verify his or her presence by subsequently decoding the private key that was destroyed by a prior use. One of ordinary skill in the art would not be lead to change Trostle's invention by introducing a process that contradicts Trostle's explicit teachings, absent a specific suggestion to the contrary.

Asay teaches the destruction of a private, *and subsequent reconstruction* of the key in order to form the user's private key. The Examiner references a sentence in Asay that directs the destruction of a private key (Asay, column 30, lines 55-57). This sentence, however, is prefaced with "the corresponding private key is stored in a safe place in the subscriber's system" (Asay, column 30, lines 53-54), and followed with "[t]he subscriber mechanism 106 then unwraps the private key stored away for use in the event that a certificate is issued based on the standby application" (Asay, column 31, lines 14-17). The term "unwrap", as commonly used in the art, is synonymous with "decrypted". That

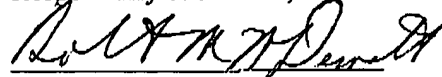
is, Asay destroys a copy of the private key only for the duration required to determine whether the (new) certificate is going to be issued. Once the certificate is issued, the user's system "unwraps" the private key for subsequent use, consistent with conventional systems, and particularly Trostle, that are specifically designed to make the security process "transparent to the user". Anyone who uses the subscriber system of Asay after the private key is unwrapped will be able to access the user's private key, will be able to access encrypted files, and will be able to sign documents as the user.

It is particularly significant to note that the referenced process of Asay also occurs independent of the user. When the subscriber system of Asay notes that a certificate is due to expire, it initiates an automated process to renew the certificate (Asay, column 29). Only if the certificate has expired, and this first automated process fails, is the second automated process invoked that initiates the standby application. This second automated process occurs independent of a user interaction. The subscriber system automatically initiates a standby application that includes a public-private key pair that is "different from any other on the subscriber's system" (Asay, column 30, lines 51-53). This private key is not the "user's private key", per se, but only becomes the user's private key after the standby application is approved by the certifying authority. After the standby application is approved, this private key is subsequently unwrapped to form the user's private key that is used for encryption and/or digital signing. Once the key becomes the user's private key, it is not destroyed. As with Trostle, Asay's process will work, and will continue to provide an unwrapped private key at the subscriber system, independent of whether the user is physically present at the subscribing system.

Based on Asay's specific teaching of unwrapping the private key that is stored at the user/subscriber system after the use of the private key is authorized, one of ordinary skill in the art would not be lead to the Applicant's specific teaching of deleting the user's private key after each use.

Because neither Trostle nor Asay, individually or collectively, teach or suggest transmitting an encoded user key to a terminal for subsequent decoding into a user key that is used and then destroyed, the Applicant respectfully requests the Examiner's reconsideration of the rejection of claim 5-8 under 35 U.S.C. 103(a) over Trostle in view of Asay.

Respectfully submitted,



Robert M. McDermott, Esq.

Reg. No. 41,508

804-493-0707

CERTIFICATE OF MAILING OR TRANSMISSION

It is hereby certified that, on the date shown below, this correspondence is being:

☐ deposited with the United States Postal Service with sufficient postage as first-class mail in an envelope addressed to: ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, DC 20231.

☒ transmitted by facsimile to the United States Patent and Trademark Office at 703-746-7239.

On 29 July 2002

By

